

Fraud Management Internal Design

Change Log

Name:	Date:	Description:
ccatlin		Fleshed out and added Appendix information...
ccatlin		Added Greg's pseudo code for Fraud Rules Engine Thanks Greg!

1. Introduction

Fraud management will be an ongoing development, things will be continually added as we learn more, gain a transaction history and fill in any possible holes we find along the way. In this document you will find a listing of all the current checks we envision at the moment, the rules associated with each check, the pseudo code concerning the code we expect to write and the Appendix sections which include:

Appendix A ... External Architecture and Process...
 Appendix B ... Fraud Management generated events/subjects...
 Appendix C ... Fraud Rules Engine Pseudo Code...
 Appendix D ... Future Fraud Management Ideas and Possible Implementation...
 Appendix E ... Projected Timeline...
 Appendix F ... Potential Small to Medium Merchant fraud checks:
 Appendix G ... Types of Fraud Perpetrators...

2. Fraud Module Checks

A note on notation: to keep the symmetry of the document, rules which may be delayed are marked with an asterix (*).

2.1. Physical data checks for all customers:

2.1.1. Standard customer fraud checks:

There are no standard checks at this time.

2.1.2. Physical data fraud checks:

All outcomes are true or false and assigned weighted scores according to rule severity.
 Exceptions are generated for rules based on a level of severity.
 Most rules here do not apply to international.

2.1.2.1. Validity of physical data:

- (2A) Check for valid address...outcome true or false(OTF)
- (3A) Check for valid city...outcome true or false(OTF)
- (4A) Check for valid state...outcome true or false(OTF)
- (5A) Check for valid postal code...outcome true or false(OTF)
- (6A) Check valid phone number...OTF
- (7A) Check valid email address...OTF
- (8A) Check valid owner of email address...OTF
- (9A) Check validity Buyer name...OTF

2.1.2.2. Consistency of physical data:

- (10A) Check valid address compared to the given postal code...OTF
- (11A) Check valid Buyer name compared to phone number...OTF
- (12A) Check valid Buyer name compared to address...OTF

2.1.2.3. Blacklist of physical data:

- (13A) Check valid Buyer name against a known black list...OTF
- (14A) Check valid Buyer addresses against a known black list...OTF
- (15A) Check valid Buyer email address against a known black list...OTF
- (16A) Check valid credit card # against a known black list...OTF
- (17A) Check ID against static gray list of pending cases.
- (18A) Check valid Buyer name against a known gray list...OTF
- (19A) Check valid Buyer addresses against a known gray list...OTF
- (20A) Check valid Buyer email address against a known gray list...OTF
- (21A) Check valid credit card # against a known gray list...OTF

2.2. Physical Cardholder(Buyer) data checks:

2.2.1. Standard Buyer fraud checks:

AVS – Checks numerical elements of address such as house number, apartment number and zip code.
Done by Paymentech for us in the US.

Paymentech forwards the AVS codes listed below to be checked and handled by us.

- X (full match)
- Y (full minus ZIP extension)
- W(9 digit zip only)
- Z(5 digit zip only)
- A (address only)
- N (nothing matched)

S (issuer nonparticipant)
U (address unavailable)
E (input error)
_(not performed)
?? (system error)
N1 (other input error)
N2 (other input error)

(1B) AVS rule: Check for AVS code...possible outcome listed above.

2.2.2. Physical data fraud checks:

The physical data checks listed in section 2.1.

2.2.3. New data to ask Cardholder(Buyer) to provide:

(17B) Check valid CVV2 or CVC...OTF
(18B) Check valid name of bank who issued card...OTF

2.3. Physical Merchant(Seller) data checks:

2.3.1. Standard:

No Standard checks for Merchants
Possible Equifax Scoring and possible Credit check.

2.3.2. Superset physical data fraud checks:

All outcomes are true or false and assigned weighted scores according to rule severity.
Exceptions are generated for rules based on a level of severity.
Most rules here do not apply to international.

All of the generic customer physical data checks.

(13S) Check valid Seller bank account against a known black list.
(14S) Check valid bank name.
(15S) Check valid bank routing number.
(17S) Check postal code matches area code for fax number.

2.3.3. New data to ask Merchant(Seller) to provide:

(18S) Check valid Social Security number
(19S) Check valid Business Tax ID

2.4. Transaction Modeling Checks:

2.4.1. Velocity Checks

The velocity checks all are of the form “number per time” or similar. This can be computed either by fixing a time interval and measuring the number of events, or by fixing a number of events and measuring the time interval, or both. The former is more intuitive and less storage intensive. The latter will catch fraudsters with a lower false positive rate.

A similar distinction can be drawn when measuring a ratio of events: how many event A s occur for each N event B s. Event b is assumed to occur every time A occurs. For example, event B is card declined and event A is card declined due to wrong CVV2. We can count events A and B until B reaches some preset number- this is analogous to counting events in a time interval. We can also count both types of events until the count of A reaches some preset number. This is analogous to measuring the time interval for a set number of events.

2.4.1.1. By Transaction Volume

- (1VTV) Check # of transactions by credit card number per time
- (2VTV) Check # of transactions by buyer name per time
- (3VTV) Check # of transactions by first 12 digits of credit card number per time
- (4VTV) Check # of transactions by bin # per time
- (5VTV) Check # of transactions by seller per time

- (6VTV) Check # of transactions by credit card number per time by seller
- (7VTV) Check # of transactions by buyer name per time by seller
- (8VTV) Check # of transactions by first 12 digits of credit card number per time by seller
- (9VTV) Check # of transactions by bin # per time by seller

- (10VTV) Check # of transactions by credit card number per seller volume by seller
- (11VTV) Check # of transactions by buyer name per seller volume by seller
- (12VTV) Check # of transactions by first 12 digits of credit card number per seller volume by seller
- (13VTV) Check # of transactions by bin # per seller volume by seller
- (14VTV) Check # of transactions by Card type (MC/VISA) per seller volume by seller

- (15VTV) Check # of transactions by OS per total transactions by time.
- (16VTV) Check # of transactions by Browser per total transactions by time.
- (17VTV) Check # of transactions by Buyer ID by time.

<Still adding...more to be decided...>

2.4.1.2. By Transaction Amount

- (1VTA) Check \$ of transactions by credit card number per time
- (2VTA) Check \$ of transactions by buyer name per time
- (3VTA) Check \$ of transactions by first 12 digits of credit card number per time
- (4VTA) Check \$ of transactions by bin # per time
- (5VTA) Check \$ of transactions by seller per time

- (6VTA) Check \$ of transactions by credit card number per time by seller
- (7VTA) Check \$ of transactions by buyer name per time by seller

(8VTA) Check \$ of transactions by first 12 digits of credit card number per time by seller
(9VTA) Check \$ of transactions by bin # per time by seller

(10VTA) Check \$ of transactions by credit card number per seller volume by seller
(11VTA) Check \$ of transactions by buyer name per seller volume by seller
(12VTA) Check \$ of transactions by first 12 digits of credit card number per seller volume by seller
(13VTA) Check \$ of transactions by bin # per seller volume by seller
(14VTA) Check \$ of transactions by Card type (MC/VISA) per seller volume by seller

2.4.1.3. By Decline Rate

(1VDR) Check # of declines by credit card number per time.
(2VDR) Check # of declines by buyer name per time.
(3VDR) Check # of declines by first 12 digits of credit card number per time.
(4VDR) Check # of declines by bin # per time.
(5VDR) Check # of declines by seller per time.

(6VDR) Check # of declines by credit card number per time by seller.
(7VDR) Check # of declines by buyer name per time by seller.
(8VDR) Check # of declines by first 12 digits of credit card number per time by seller.
(9VDR) Check # of declines by bin # per time by seller.

(10VDR) Check # of declines by credit card number per seller volume by seller.
(11VDR) Check # of declines by buyer name per seller volume by seller.
(12VDR) Check # of declines by first 12 digits of credit card number per seller volume by seller.
(13VDR) Check # of declines by bin # per seller volume by seller.
(14VDR) Check # of declines per seller volume by seller.

2.4.1.4. By Error code specific decline rate

(15VDR) Check # of declines due to CVV2 per total declines
(16VDR) Check # of declines due to Authorization code 522 per total declines
(17VDR) Check # of declines due to Authorization code 531 per total declines
(18VDR) Check # of declines due to Authorization code 210 per total declines
(19VDR) Check # of declines due to CVV2 per total declines by seller id
(20VDR) Check # of declines due to Authorization code 522 per total declines by seller id
(21VDR) Check # of declines due to Authorization code 531 per total declines by seller id
(22VDR) Check # of declines due to Authorization code 210 per total declines by seller id
(23VDR) Check # of declines due to CVV2 per total declines by phone number
(24VDR) Check # of declines due to Authorization code 522 per total declines by phone number
(25VDR) Check # of declines due to Authorization code 531 per total declines by phone number
(26VDR) Check # of declines due to Authorization code 210 per total declines by phone number
(27VDR) Check # of declines due to CVV2 per total declines by fax number
(28VDR) Check # of declines due to Authorization code 522 per total declines by fax number
(29VDR) Check # of declines due to Authorization code 531 per total declines by fax number
(30VDR) Check # of declines due to Authorization code 210 per total declines by fax number
(31VDR) Check # of declines due to CVV2 per total declines by BIN
(32VDR) Check # of declines due to Authorization code 522 per total declines by BIN

- (33VDR) Check # of declines due to Authorization code 531 per total declines by BIN
- (34VDR) Check # of declines due to Authorization code 210 per total declines by BIN

2.4.2. Ticket Value Checks

- (1TV) Check amount of transaction.
- (2TV) Check amount of each item in a multi-item transaction.

<Still adding...more to be decided...>

2.5. Tertiary Historical Pattern Modeling Checks (against global data) :

All out comes are weighted according to rule severity.
Exceptions are generated for rules based on a level of severity.
Appropriate counts are kept for each of the variables associated with these rules.

The 9 digit zip code rules are, of course, only in effect if we gather that information.

- (12THP) Check one name showing up associated to multiple physical addresses
- (13THP) Check one name showing up associated to multiple phone numbers
- (14THP) Check one name showing up associated to multiple 5 digit postal codes
- (15THP) Check one name showing up associated to multiple email addresses
- (16THP) Check one name showing up associated to multiple fax numbers
- (17THP) Check one name showing up associated to multiple credit card numbers

- (21THP) Check one address showing up associated to multiple names
- (23THP) Check one address showing up associated to multiple phone numbers
- (24THP) Check one address showing up associated to multiple 5 digit postal codes
- (25THP) Check one address showing up associated to multiple email addresses
- (26THP) Check one address showing up associated to multiple fax numbers
- (27THP) Check one address showing up associated to multiple credit card numbers

- (31THP) Check one phone number showing up associated to multiple names
- (32THP) Check one phone number showing up associated to multiple physical addresses
- (34THP) Check one phone number showing up associated to multiple 5 digit postal codes
- (35THP) Check one phone number showing up associated to multiple email addresses
- (36THP) Check one phone number showing up associated to multiple fax numbers
- (37THP) Check one phone number showing up associated to multiple credit card numbers

- (41THP) Check one 9 digit zip code showing up associated to multiple names
- (42THP) Check one 9 digit zip code showing up associated to multiple physical addresses
- (43THP) Check one 9 digit zip code showing up associated to multiple phone numbers
- (45THP) Check one 9 digit zip code showing up associated to multiple email addresses
- (46THP) Check one 9 digit zip code showing up associated to multiple fax numbers
- (47THP) Check one 9 digit zip code showing up associated to multiple credit card numbers

(51THP) Check one email address showing up associated to multiple names
 (52THP) Check one email address showing up associated to multiple physical addresses
 (53THP) Check one email address showing up associated to multiple phone numbers
 (54THP) Check one email address showing up associated to multiple 5 digit postal codes
 (56THP) Check one email address showing up associated to multiple fax numbers
 (57THP) Check one email address showing up associated to multiple credit card numbers

(61THP) Check one fax number showing up associated to multiple names
 (62THP) Check one fax number showing up associated to multiple physical addresses
 (63THP) Check one fax number showing up associated to multiple phone numbers
 (64THP) Check one fax number showing up associated to multiple 5 digit postal codes
 (65THP) Check one fax number showing up associated to multiple email addresses
 (67THP) Check one fax number showing up associated to multiple credit card numbers

(71THP) Check one credit card number showing up associated to multiple names
 (72THP) Check one credit card number showing up associated to multiple physical addresses
 (73THP) Check one credit card number showing up associated to multiple phone numbers
 (74THP) Check one credit card number showing up associated to multiple 5 digit postal codes
 (75THP) Check one credit card number showing up associated to multiple email addresses
 (76THP) Check one credit card number showing up associated to multiple fax numbers

(42 total, for the rules counters.)

This list is more easily viewed as a table, with presumed keys on the left and associated multiples on top.

Many One	name	address	phone	Zip (5)	Email	Fax	Card #
name		X	X	X	X	X	X
address	X		X	X	X	X	X
phone	X	X		X	X	X	X
Zip (9)	X	X	X		X	X	X
Email	X	X	X	X		X	X
Fax	X	X	X	X	X		X
Card #	X	X	X	X	X	X	

2.6.Bogus data Checks

Check for keyboard patterns...such as asdf.

Check for series patterns such as 1234.

Check for same keys multiple times and variations such as 11111 or MMMMM.

<Still adding...more to be decided...>

2.7.Internal Physical data checks – fingerprint user:

Standard:

Track remote IP address
Track remote Host IP address
Track Remote Host Name
Track Remote Name

<Still adding...more to be decided...>

2.8.Internal Web Site data checks:

Check # of times a Seller logs on to site.
Check # of times a Seller changes email.
Check # of times a Seller changes billing name.
Check # of times a Seller changes url.
Check # of times a Seller changes bank name.
Check # of times a Seller changes bank account number.
Check # of times a Seller changes routing number.

<Still adding...more to be decided...>

2.9.Internal Credit Card data checks:

Track/Check # of Retrieval Requests for cardholder.
Track/Check # of charge backs for cardholder.
Check time of Transactions.
Check if International.
Check Response Reason codes from Paymentech.

<Still adding...more to be decided...>

Appendix A - External Process and Architecture...

Buyer(Cardholder) high level overview of the fraud management process...

Buyer(Cardholder) clicks on billpoint button...billpoint collects form data or uses existing data...form and transaction data is sent to fraud management...buyer and transaction data is either processed by fraud module right away or remedial action is taken afterwards or maybe even a mix of both depending on the model we choose...if the fraud system detects the hint of fraud, a case number is created, data is transferred to the case, the case is presented to an individual for looking into and we call and email the individuals involved to discern if there is indeed fraud.

Seller(Merchant) high level overview of the fraud management process...

Seller(merchant) registers with the billpoint system through an application process...billpoint collects form data... form data is sent to fraud management... seller data is either processed by fraud module right away or remedial action is taken afterwards or maybe even a mix of both depending on the model we choose... if

the fraud system detects the hint of fraud a case number is created, data is transferred to the case, the case is presented to an individual for looking into and we call and email the individuals involved to discern if there is indeed fraud. The Seller may also be involved during the Buyer fraud management process...

Overall Architecture thoughts...

Fraud Module(s) are running in background waiting for these possible tibco events/subjects...

- Bp.BPENV.newCustomer
- Bp.BPENV.preAuthTran
- Bp.BPENV.postAuthTran
- Bp.BPENV.customerInfoChg
- Bp.BPENV.customerLogon

<Still adding...more to be decided...>

When one of these events is fired the appropriate fraud services are rendered.

Current fraud module processing concepts...

All fraud checks will produce a score depending on the outcome of the check. All scores will be tallied and the total score will be evaluated and a case will be assigned if the evaluation shows a level consistent with fraud. In the event a case is assigned, a customer service fraud rep will be notified and the case transferred to them. Currently in the first version this case processing will be handled by email. In future versions there will be a gui screen/app capable of presenting and processing fraud cases.

Besides the above processing, certain designated fraud checks will also emit exceptions/events. These are needed by external services in such cases where other billpoint services need to be notified and act accordingly. As in the examples where the CVV2 number is incorrect...the name does not match the presented email, phone and address or the card number has been identified as fraudulent. Examples of things that may need to happen by other billpoint services when hearing these events may be putting the transaction on hold, de-authorizing the transaction or putting a buyer or seller account on hold.

Goals to be kept in mind during fraud module programming...

Generic rules engines are created to handle as much as possible, inserting different data types and data sets into the generic engine for processing.

Module is database driven, all meta data is stored in the database and possibly cached during module use for speed.

A generic weight engine and exception engine is created to handle requests by the fraud module for these services.

Appendix B – Fraud Management generated events/subjects...

<to be decided...>

Appendix C – Fraud Rules Engine Pseudo Code...

Events A per events B

Rule Id	Entries in table	What to count	Group numerator or by	Restrict numerator or to	Group denominator or by	Restrict denominator or to	Max numerator	Max denominator	Fraud weight
	Table name	(1 or numeric column name)	Column name	Column name and value	Column name	Column name and value	long	long	long
1	transaction	\$ amount	BIN #	----	Seller ID	-----	500	5000	3
2	transaction	1	BIN #	----	Seller ID	-----	5	100	7

The first rule says “if a seller has more than \$500 out of any \$5000 coming from the same BIN number, give the transaction a fraud weight of 3.”

The second rule says “if a seller has more than 5 out of any 100 attempted transactions coming out of the same BIN number, give the transactions a fraud weight of 7.”

Rule Id	Numerator grouping value	Denominator grouping value	Numerator count	
1	6011	12 (Abby)	300	
2	4128	15 (Max)	16	

Rule Id		Denominator grouping value	Denominator count	
1		12 (Abby)	1900	
2		15 (Max)	40	

The first item says “out of Abby’s last \$1900 in sales, \$300 have been with discover card.”
The second item says “out of Max’s last 40 sales, 16 have been with Citibank Visa cards”

Events A per time

Rule Id	Entries in table	What to count	Group numerat or by	Restrict numerat or to	Max numerator	Max denominator	Fraud weight to transaction	Fraud weight to seller
	Table name	(1 or numeric column name)	Column name	Column name and value	long	long	long	
3	transacti on	\$ amount	BIN #	----	5000	43200	5	10
4	transacti on	1	BIN #	----	5	120	7	8

The first rule says “if a seller has more than \$5000 in transactions per month (43200 minutes), give the transaction a fraud weight of 5 and the seller a fraud weight of 10.”

The second rule says “if a seller has more than 5 transactions with the same BIN number in 2 hours, give the transaction a fraud weight of 7 and the seller a fraud weight of 8.”

Rule Id	Numerator grouping value	Denominator grouping value	Numerator count	
3	6011	12 (Abby)	300	
4	4128	15 (Max)	6	
4	6011	15 (Max)	2	

Rule Id		Denominator grouping value		Denominator count
3		12 (Abby)		135
4		15 (Max)		30
4		15 (Max)		30

The first item says “Abby has run \$300 in transactions with the discover card in the last 135 minutes.”

The second item says “May has done 6 transactions with Citibank Visa cards in the last half hour.”

Pseudocode:

On initialization

- For all rules,
 - Load the rule into memory

On transaction, new account, or change account info

- For all rules in memory
 - If the transaction (or other) matches the restrictions
 - Test the rule

To test a rule

- If (can find the pair (rule Id, denominator group))
 - Increment denominator count
- Else
 - Create such a pair
- If denominator count is above threshold
 - For all numerator counts with this denom.
 - Set to zero.
 - Set denominator count to one.
- If (can find the triple of ruleId, numerator group, denominator group)
 - Increment numerator count
- Else
 - Create such a triple.
- If (numerator count is above threshold)
 - Throw Ex.

Appendix D - Future Fraud Management Ideas and Possible Implementation...

- Track merchant average ticket price.
- Track Merchant most common ticket price.
- Track Merchants most common item purchased.
- Use Equifax scoring.
- Run Credit checks on Merchants.
- Associate fraud risks with SIC codes – add to scoring model.
- Track if shipping address changes during shipping process.
- Give customer service folks a list of data to verify to validate person during processing.
- Give fraud weighting to transactions where ship to does not match bill to address.
- Check into getting Visa and MC terminated merchant file.
- Add different checks/rules for physical and virtual goods.
- Give fraud weighting to certain ISPs, IP addresses, Email sources, Browsers, OS s, and so on.

Appendix E - Projected Timeline

•Week of March 15th...

- Research Fraud Management space
- Research Fraud Management software
- Create Initial Fraud Management Coverage Docs
- Negotiate short term partnership/engagement with HNC
- Research fraud internet sites
- Prepare for HNC engagement

•Week of March 22nd...

- Review Paymentech documents (chargeback manual, fraud aware docs)
- Meet/Start work with HNC and define fraud business rules and pseudo code to be used in our fraud system.
- Meet with Paymentech.
- Design Current Fraud management rule set
- Create fraud design doc and fraud coverage matrix
- Develop how Equifax should be used. Product group meeting.
- Explore integration of HNC/Equifax verification system and any other fraud issues.

•Week of March 29th...

- Start to Finalize marketing relationships with HNC.
- Design/start coding Fraud event ratio engine
- Design/start coding Fraud event frequency engine
- Design/start coding Fraud Physical data rule set
 - Buyers
 - Sellers
 - Blacklist
 - External Database checks

•Week of April 5th...

- Design/start coding AVS engine

- Implement fraud case creation process/software and continued rule code tuning and testing by implementers

•Week of April 12th...

- Finish Fraud Management implementation started at the end of the week of March 29th and April 5th

- Start internal testing

•Week of April 19th...

- Finish left over odds and ends...

- Polish code

- Start External testing...

Appendix F – Potential Small to Medium Merchant fraud checks:

<To be added from HNC list...>

Appendix G - Types of Fraud Perpetrators:

Make sure we cover these in our model either through rules, profiling or neural...

Ways to get the credit card number.

For both buyer fraud and collusionary fraud, the fraudster needs to obtain a credit card number and related information from somewhere. The following are devious ways to get credit card numbers, roughly in order of sophistication.

- a use own card.
- b use friend or relative's card.
- c steal a wallet.
- d1 generate card numbers
- d2 get other card info alone. (eg: carbon)
- e get card info with other personal info. (eg- screen the mail or the trash.)
- f get a real card for a fake identity.
- g get a real card for a stolen identity.
- h pretend to be a merchant, save the information, reject all cards.
- i pretend to be a merchant, use the information as the user types it in. (forward it directly to billpoint or some other merchant.)
- j pretend to be billpoint. (forward as in h or i.)

There is a direct relationship between the first 7 of these items and the classes of fraudsters noted in the Paymentech brochure. (a and b are typical of weekend cons, c is typical of card cons, and e through h are a portion of what experienced cons use.)

Billing scams

- a overcharge. (price told to buyer is not same as price told to billpoint.)
- b seller enters data for buyer. (avoid proper buyer screening.)

Scams in the sending of items, to defraud buyer.

- a send nothing
- b send empty box or clearly different good
- c send defective goods, but not obviously so. (think digital goods here.)
- d illegal goods.
- e misrepresent legal deal to buyer.
- f porn and other socially unpopular goods.

(This last one is not fraud, and we should avoid becoming a censor if at all possible.)

Scams in the sending of goods, to confuse us.

- a send to a buddy.
- b send to a dead address of some sort.
- c send no signature required. steal it.
- d send to someone known to be on vacation. (easy if the site sells vacation info.)
- e lie about where it is being sent.

Cooperative Scams.

- a buyer knows to deny charge after seller gets paid.
- b buyer denies receipt of goods.
- c seller enters card numbers for mythical buyers (obtained somehow. see top.)

Ways to avoid detection

- a 12 guys in a house to answer phone lines (buyer and seller side.)
- b claim to be selling something clean. (eg: bibles. diskspace. ...)
- c split across several merchants and escrow services.
- d act as seller. Many of the standard checks are written to protect merchants from fraudulent buyers, and would fail.
- e single fraudster can have multiple identities.
- f skip out. (bp should not assume that it can always contact both parties after fraud has been detected.)
- g half skip out. (act as both buyer and seller. buyer disappears "with goods." seller pleads ignorance and splits the cost of the chargeback with billpoint. Net profit of one half of the charged amount.)

Text_r-1

VTV Rule 2002: The total number of transactions from a single SellerId can have at most 3 transactions from any given CardNumber per 1000 transactions .

ITV Rule 2003: The total number of transactions from a single BinNumber can have at most 3 transactions from any given CardNumber per 100 transactions .

VTV Rule 2004: The total number of transactions from a single SellerId can have at most 3 transactions from any given BuyerId per 100 transactions .

Rule 2005: The total number of transactions from a single SellerId can have at most 3 transactions from any given Cvv2Resp per 100 transactions . *

Rule 2006: The total number of transactions from a single SellerId can have at most 3 transactions from any given AvsResp per 100 transactions . *

Rule 2007: The total number of transactions from a single SellerId can have at most 3 transactions from any given AuthResp per 100 transactions . *

7V Rule 2011: The total dollars of transactions from a single SellerId can have at most 1000 dollars of transactions from any given BuyerId per 10000 dollars of transactions .

6VTA Rule 2012: The total dollars of transactions from a single SellerId can have at most 1000 dollars of transactions from any given CardNumber per 10000 dollars of transactions .

9VTA Rule 2013: The total dollars of transactions from a single BinNumber can have at most 1000 dollars of transactions from any given CardNumber per 10000 dollars of transactions .

7 Rule 2014: The total dollars of transactions from a single SellerId can have at most 1000 dollars of transactions from any given BuyerId per 10000 dollars of transactions .

Rule 2015: The total dollars of transactions from a single SellerId can have at most 1000 dollars of transactions from any given Cvv2Resp per 10000 dollars of transactions . *

Rule 2016: The total dollars of transactions from a single SellerId can have at most 1000 dollars of transactions from any given AvsResp per 10000 dollars of transactions . *

Rule 2017: The total dollars of transactions from a single SellerId can have at most 1000 dollars of transactions from any given AuthResp per 10000 dollars of transactions . *

Text_r-1

Rule 2021: The total number of transactions from a single SellerId can have at most 3 transactions from any given AuthResp per 100 transactions .

Rule 2022: The total number of transactions from a single BuyerId can have at most 3 transactions from any given AuthResp per 100 transactions .

Rule 2023: The total number of transactions from a single CardNumber can have at most 3 transactions from any given AuthResp per 100 transactions .

Rule 2024: The total number of transactions from a single BinNumber can have at most 3 transactions from any given AuthResp per 100 transactions .

Rule 2041: The total number of transactions from a single SellerId can have at most 3 transactions from any given Cvv2Resp per 100 transactions .

Rule 2042: The total number of transactions from a single BuyerId can have at most 3 transactions from any given Cvv2Resp per 100 transactions .

Rule 2043: The total number of transactions from a single CardNumber can have at most 3 transactions from any given Cvv2Resp per 100 transactions .

Rule 2044: The total number of transactions from a single BinNumber can have at most 3 transactions from any given Cvv2Resp per 100 transactions .

Rule 2051: The total number of transactions from a single SellerId can have at most 3 transactions from any given AvsResp per 100 transactions .

Rule 2052: The total number of transactions from a single BuyerId can have at most 3 transactions from any given AvsResp per 100 transactions .

Rule 2053: The total number of transactions from a single CardNumber can have at most 3 transactions from any given AvsResp per 100 transactions .

Rule 2054: The total number of transactions from a single BinNumber can have at most 3 transactions from any given AvsResp per 100 transactions .

Rule 2031: The total number of transactions can have at most 3 transactions from any given AuthResp per 100 transactions .

Rule 2032: The total number of transactions can have at most 3 trans

Text_r-1

actions from any given AvsResp per 100 transactions .

Rule 2033: The total number of transactions can have at most 3 transactions from any given Cvv2Resp per 100 transactions .

Rule 2001: The total number of transactions from a single SellerId can have at most 5 transactions from any given BinNumber per 100 transactions .

Rule 1002: The total number of transactions from a single BuyerId and SellerId can have at most 2 transactions per 60 minutes.

Rule 1003: The total number of transactions from a single BinNumber and SellerId can have at most 2 transactions per 60 minutes.

Rule 1004: The total number of transactions from a single BuyerId can have at most 2 transactions per 60 seconds.

Rule 1005: The total number of transactions from a single BinNumber can have at most 2 transactions per 10 seconds.

Rule 1006: The total number of transactions from a single CardNumber can have at most 2 transactions per 100 seconds.

Rule 1011: The total dollars of transactions from a single CardNumber and SellerId can have at most 1000 dollars of transactions per 24 hours.

Rule 1012: The total dollars of transactions from a single BuyerId and SellerId can have at most 1000 dollars of transactions per 24 hours.

Rule 1013: The total dollars of transactions from a single BinNumber and SellerId can have at most 1000 dollars of transactions per 60 minutes.

Rule 1014: The total dollars of transactions from a single BuyerId can have at most 1000 dollars of transactions per 24 hours.

Rule 1015: The total dollars of transactions from a single BinNumber can have at most 10000 dollars of transactions per 10 days.

Rule 1016: The total dollars of transactions from a single CardNumber can have at most 1000 dollars of transactions per 24 hours.

Rule 1021: The total number of transactions from a single AuthResp and CardNumber can have at most 3 transactions per 24 hours.

Rule 1022: The total number of transactions from a single AuthResp and BinNumber can have at most 3 transactions per 24 hours.

Rule 1023: The total number of transactions from a single AuthResp and SellerId can have at most 3 transactions per 24 hours.

Text_r-1

Rule 1024: The total number of transactions from a single AuthResp and BuyerId can have at most 3 transactions per 24 hours.

Rule 1031: The total number of transactions from a single AvsResp and CardNumber can have at most 3 transactions per 24 hours.

Rule 1032: The total number of transactions from a single AvsResp and BinNumber can have at most 3 transactions per 24 hours.

Rule 1033: The total number of transactions from a single AvsResp and SellerId can have at most 3 transactions per 24 hours.

Rule 1034: The total number of transactions from a single AvsResp and BuyerId can have at most 3 transactions per 24 hours.

Rule 1041: The total number of transactions from a single Cvv2Resp and CardNumber can have at most 3 transactions per 24 hours.

Rule 1042: The total number of transactions from a single Cvv2Resp and BinNumber can have at most 3 transactions per 24 hours.

Rule 1043: The total number of transactions from a single Cvv2Resp and SellerId can have at most 3 transactions per 24 hours.

Rule 1044: The total number of transactions from a single Cvv2Resp and BuyerId can have at most 3 transactions per 24 hours.

Rule 1001: The total number of transactions from a single CardNumber and SellerId can have at most 2 transactions per 60 minutes.